Strategy Research Project

DoD Installation Energy Security: Evolving to a Smart Grid

by

Colonel Brian L. Magnuson
United States Marine Corps

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-03-2012	Strategy Research Project	

4. TITLE AND SUBTITLE
DoD Installation Energy Security: Evolving to a Smart Grid

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Brian L. Magnuson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Thomas J. Sexton
Department of Military Strategy,
Planning, & Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution: A

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Department of Defense (DoD) installations are reliant on civilian infrastructure for electrical power. As DoD and private industry evolve their energy production, distribution, and consumption apparatus, does it make sense for DoD installations to develop smart grids and what are the various risks and advantages to participating in smart grid development? DoD installations face many risks to the security of their future source of electrical power: physical, fiscal, natural, and cyber. Recent federal mandates dictate increased use of renewable energy resources, use of advanced electrical meters, and higher energy performance standards for new and existing DoD buildings. The primary methods to achieving these mandates are the increased use of renewable resources and smart grid technologies. The increased use of renewable resources and smart grid technologies is not without risk. Renewable energy resources are inconsistent, and current technology does not allow for energy storage. Smart grid technologies are vulnerable to cyber-attack and lack standardization. There are definitive risks to the DoD installation and its electrical infrastructure participating in smart grid development but the balance of risk versus gain can be found.

15. SUBJECT TERMS
Electricity, Electrical Grid, Cyber Security, Energy Policy

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	28	

USAWC STRATEGY RESEARCH PROJECT

DOD INSTALLATION ENERGY SECURITY: EVOLVING TO A SMART GRID

by

Colonel Brian L. Magnuson
United States Marine Corps

Colonel Thomas J. Sexton
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Brian L. Magnuson

TITLE: DoD Installation Energy Security: Evolving to a Smart Grid

FORMAT: Strategy Research Project

DATE: 20 March 2012 WORD COUNT: 5,479 PAGES: 28

KEY TERMS: Electricity, Electrical Grid, Cyber Security, Energy Policy

CLASSIFICATION: Unclassified

Department of Defense (DoD) installations are reliant on civilian infrastructure for electrical power. As DoD and private industry evolve their energy production, distribution, and consumption apparatus, does it make sense for DoD installations to develop smart grids and what are the various risks and advantages to participating in smart grid development? DoD installations face many risks to the security of their future source of electrical power: physical, fiscal, natural, and cyber. Recent federal mandates dictate increased use of renewable energy resources, use of advanced electrical meters, and higher energy performance standards for new and existing DoD buildings. The primary methods to achieving these mandates are the increased use of renewable resources and smart grid technologies. The increased use of renewable resources and smart grid technologies is not without risk. Renewable energy resources are inconsistent, and current technology does not allow for energy storage. Smart grid technologies are vulnerable to cyber-attack and lack standardization. There are definitive risks to the DoD installation and its electrical infrastructure participating in smart grid development but the balance of risk versus gain can be found.

DOD INSTALLATION ENERGY SECURITY: EVOLVING TO A SMART GRID

Hurricane Katrina struck the Gulf Coast in August of 2005, plunging 2.7 million people into electrical darkness as the hurricane knocked the aging electrical distribution network offline.[1] It only took a few short days to restore power to Florida residents, however it took upwards of a month to restore power to more than 200,000 people in the hardest hit areas. During the ensuing time period United States military forces, both active duty and National Guard, joined recovery efforts using military installations throughout the gulf coast. Many of the military installations were without electrical power. The electrical grid disruptions caused by Hurricane Katrina exposed the security risks associated with Department of Defense (DoD) installations reliance on civilian infrastructure for electrical power.

The same month Hurricane Katrina struck, Congress passed the Energy Policy Act of 2005 (EPA2005) establishing a new foundation for federal government energy management initiatives.[2] EPA2005 and follow-on legislation like The Energy Independence and Security Act of 2007 (EISA2007), and numerous National Defense Authorization Acts (NDAA) included new or higher standards for energy performance of buildings, increased use of renewable energy resources, and mandates for the DoD to use advanced electrical meters to reduce electricity use.[3] These mandates require significant efforts and resources to implement.

Around the same time, US energy companies began evolving the aging electrical distribution system, or grid, with new technologies to make the grid more efficient and reliable. This evolving system is referred to as the “Smart Grid.”[4] As DoD and private industry evolve their energy production, distribution, and consumption apparatus, does it

make sense for DoD installations to develop smart grids and what are the various risks and advantages to participating in smart grid development?

The purpose of this paper is to explore the relationships and highlight the risks surrounding DoD electricity initiatives, federally mandated energy policies, and the evolving North American electrical distribution system. First, this paper will highlight recent energy policies affecting DoD installations. Next, the paper will broadly define the North American electrical distribution system, trace its evolution, and explain the basic principles behind the electrical distribution system, or grid. Once the basic electrical grid is defined, this paper will describe the planned future of the electrical distribution system and the key components of that system. Having outlined the future of the electrical system, this paper will identify DoD energy mandates and discuss renewable energy projects before delving into a discussion of risks to the DoD electricity supply. Next, this paper will discuss the different ways DoD installations can implement electricity policy and technology, as well as methods DoD can stimulate new electricity technology. Finally, this paper will attempt to draw some conclusions as to how or whether DoD should participate in the evolution of the electrical system.

The Department of Defense maintains 300,000 buildings and 2.2 billion square feet of space, three times the footprint of Wal-Mart and five times that of the General Services Administration.[5] The Department spends $4 billion a year on “facility energy” to power these buildings.[6] Perhaps with these realities in mind, the Energy Policy Act of 2005 and other more recent initiatives are driving the DoD to invest significantly in renewable energy resources like solar, wind, and geothermal, as well as energy efficient vehicles. The stated purpose of these investments is to meet federally mandated goals,

lower operating costs, stimulate technology, and to improve energy security against a myriad of threats: physical, fiscal, natural, and cyber.[7]

The highest levels of the federal government understand the implications of energy security. The stated purpose of the EPA2005 was "to ensure jobs for our future with secure, affordable, and reliable energy."[8] The policy gave specific guidance to federal agencies in, among other areas, building performance and renewable energy utilization. Follow-on legislation such as The Energy Independence and Security Act of 2007 directed a thirty percent reduction in federal building energy usage by 2015 (relative to 2005 levels) and mandated that new federal buildings be fossil-fuel energy free by 2030.[9] These energy efficiency and security initiatives have permeated every department in DoD as each service struggles to meet goals such as "produce or procure at least twenty five percent of electrical consumption from renewable resources by 2025."[10]

The reasons for changing the existing installation energy apparatus are diverse. One major reason is cost. In the fiscally constrained environment that the DoD operates in, utilities are a "must pay" bill. The military cannot turn out the lights, shut down the computers, or stop training for missions without creating a risk to national security. A second reason for changing the way installations use energy is for mission security. The 2008 Defense Science Board found that backup power at military installations is based on flawed assumptions of grid resiliency and not sized to accommodate new Homeland Defense missions.[11] Still another reason for the DoD energy evolution is to facilitate the change itself. The Department, with its size and purchasing power, is a great contributor to technological evolution.[12] Nuclear energy

and the internet are just two examples of innovations that began with military support. Before conducting a more detailed discussion of energy security and revolutionary energy technology, it is important first to understand the basics of the electricity industry and the electrical distribution network.

The electricity industry of today is comprised of four distinct functions: generation, transmission, distribution, and system operations.[13] Electricity is generated from either fossil fuels (coal, natural gas, or oil), nuclear, or renewable (solar, wind, biomass, ocean, hydroelectric, geothermal) resources. The most common and largest forms of electrical generation come from power plants that use fossil fuels, hydroelectric, and nuclear energy. These large power generation plants are also the most expensive to build and operate. Once the electricity is produced, it needs to be transmitted to the users. Electricity is transmitted over high-voltage, high-capacity transmission lines of various sizes to distribution locations hundreds of miles away. These high-voltage transmission lines deliver the electricity to a distribution network of substations, transformers and ultimately to the consumer for use.

Overseeing the entire process, from generation to consumption at the wall socket, is the most important part of the system -- the system operations network. The system operations network is critical to the electrical distribution system because electricity cannot be easily stored so it must be generated in anticipation of demand. Additionally, supplied electrical energy must always equal or exceed demand, a term known as balancing. In order to maintain a balanced electrical supply, generation and transmission must be monitored and controlled in real time, twenty four hours a day, to ensure a consistent and ample flow of electricity. This real time balancing requires the

cooperation and coordination of hundreds of electricity industry participants.[14] System operations manage the cooperation and coordination of industry participants. In North America, system operations for the regulation of reliability standards is divided into eight regions which include Canada and portions of Mexico. Within these individual regions there are 107 "Balancing Authorities"[15] tasked to maintain and manage North American electrical production and distribution for 334 million people over 211,000 miles of high-voltage transmission lines[16], to include 99% of the electrical energy DoD installations consume.[17] The method of electricity production and distribution in use today has evolved significantly over time but the basic premise has remained largely unchanged since its inception.

The electrical production and distribution network, or grid, traces its origins back to the late eighteen hundreds and inventor Thomas Edison. Edison would invent the first electrical distribution grid to light up a considerable stretch of Broadway in New York City.[18] From that humble beginning in December 1880, Edison and other famous names like George Westinghouse and Nichola Tesla played critical roles in the evolution and expansion of the electrical grid. While the first electrical grid was built in New York City, the grid soon expanded to other major cities like Brooklyn, Boston, and Chicago. In Chicago, Samuel Insull, one of Edison's early protégé's would take the grid and evolve it. The Chicago electrical grid would become affordable to many through economies of scale; utilizing larger and more efficient generators to lower rates and subsequently increase customer demand. Between 1899 and 1913, Commonwealth Edison of Chicago would expand paying customers from ten thousand to two hundred thousand, all while reducing rates.[19] The explosion of electricity usage and the

expansion of the grid would make its way to more rural areas of the country by the 1930's. The Tennessee Valley Authority, or TVA, was a massive jobs program during the great depression of the 1930's that is best known for being a producer of electrical power through the building of hydroelectric dams.[20] The TVA raised electrical usage in the valley from fifty percent below the U.S average to twenty five percent above the U.S. average, bringing electricity to rural America.[21] This series of independent city electrical grids continued to grow and spread throughout the country and eventually gave way to three regional interconnections that comprise the national electrical grid of today.

Throughout the expansion and evolution of the grid, the basic concepts of production and distribution remained the same. Supply must always equal or exceed demand. When demand exceeds supply, whole blocks of a city lose power (controlled load shedding) in order to prevent whole cities from losing power (catastrophic system collapse). In reality, the grid is much more complex than simple supply and demand. The grid is about reliability maintained through adequacy (over-production) and operating reliability (redundancy).[22] The grid is about managing large and small problems. In the grid generators go bad, transmission lines break, and all the while voltage and frequency control mandates for the system must be maintained. The grid is also about cracked wire insulation, frayed wires, or water leaks in underground power lines.[23] All of these challenges occur on a daily basis and are managed with little impact to the consumer, thanks to reliability.

Occasionally the challenges to the grid are catastrophic. November 9, 1965 was such a day when thirty million people lost power in the northeastern United States and southeastern Ontario, Canada due to the cascading effects of tripped high-voltage

transmission line relays.[24] New York City and Toronto were among the affected cities and some customers were without power for 13 hours.[25] Catastrophe would strike again on August 14, 2003 when fifty million people in the northeastern and midwestern U.S. and Ontario, Canada would lose power due to the cascading effects of untrimmed tree limbs contacting high-voltage transmission lines.[26] As a result of these catastrophes, much has been done to improve the reliability of the electrical grid but reliability is only part of the battle.

In addition to increasing the reliability of the grid, additional production capability fed increased electricity demand. While the pace of projected electrical demand growth decreased over the last ten years from 1.79% to 1.23%, the long term assessment remains for demand to continue to increase.[27] Complicating the long term forecast are impacts such as pending environmental regulations that could significantly affect older, more pollution generating coal powered generation plants. These environmental regulations may cause significant generator retirements or tight compliance schedules requiring generation to be brought offline for updating.[28] Aging production capability, tighter environmental regulations, renewed concerns over nuclear power, and increased demand are all elements negatively affecting long term production on the grid. These combined negative impacts are in part driving both the evolution to the smart grid and increased usage of renewable resources. Having laid out the history of the electrical grid, the forecast for electrical demand, and some factors affecting future electrical production, we will now discuss the “smart grid” and how it can contribute to DoD and the nation.

The electrical grid of today is extremely complex and resilient, operating without fault better than 99% of the time. But as demand continues to grow, efficiencies need to be found in all aspects of the electrical system: production, transmission, distribution, system operations, and consumption. Early efficiencies included awareness programs like Con Edison's "Save a Watt" program.[29] The program educates consumers and encourages them to think about what electricity they use, when they use it, and how they can reduce their overall consumption by investing in home insulation or lower voltage light bulbs. These awareness initiatives address the demand side of the problem. Legislative initiatives, like EISA2007, requiring more efficient appliances like air conditioners and refrigerators also helped slow the pace of demand.[30] Over time, the efficiency gains from these initiatives plateaued requiring additional measures to ensure sustained levels of electric reliability across the grid. The next step in evolving the electrical grid was the concept of the smart grid.

EISA2007 established a federal policy to modernize the electric utility transmission and distribution system to maintain reliability and infrastructure protection through the development of the "smart grid."[31] The term "smart grid" refers to a distribution system that allows for the flow of information from a customer's meter in two directions: both inside the house to thermostats, appliances, and other devices, and from the house back to the utility.[32] The same concept applies to industrial and commercial consumer markets. Furthermore, the smart grid includes a variety of operational and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficiency resources.[33] One goal of the smart grid is to use advanced, information-based technologies to increase power grid efficiency,

reliability, and flexibility, and reduce the rate at which additional electric utility infrastructure needs to be built. At the consumer end, the smart grid will allow appliances to be turned off or down, or operations delayed during periods of high electrical demand, or high electrical cost. This smart grid capability is known as demand response.[34] For example, a major department store chain in the Northeast outfitted all its stores with smart meters. When the balancing authority sees electrical demand nearing supply, it signals, perhaps through a curtailment service provider, for each building to institute barely perceptible changes in lighting and air conditioning temperatures to reduce the aggregate demand on the electrical system.[35] This negative generation, or negawatt, allows the electricity to be sent elsewhere.[36] Similar efficiencies can be gained through smart grid technology innovations at the distribution, transmission, and production levels. Having broadly defined what the smart grid is, now let's take a look at some of the components of smart grid.

According to the Department of Energy, the Key Technological Areas (KTA) of the smart grid are: integrated two-way communication, advanced components, advanced control methods, sensing and measuring technologies, improved interfaces and decision support, and applications of smart grid technology.[37] Integrated two-way communications rely on automatic meter reading technologies to allow two-way communications to and from the producer and the consumer. For example, in the current grid the utility company relies on consumers to call and report a power outage. In contrast, the smart grid would utilize two-way communication to allow the operators to know, at the time of loss, when a certain section of the grid was out of power.[38] Advanced components include smart devices, excess electricity storage devices

(batteries), fault tolerance, diagnostic equipment, and areas of superconductivity.[39] Advanced control methods will enable real time diagnosis and timely response to events (changes in current flow, fault location and isolation) through new methods and algorithms, significantly shortening or eliminating power outages.[40] Sensing and Measuring technologies include smart meters and the associated infrastructure, to include cyber-security, which allow the transformation of data into information.[41] In order to support the significant increase in information provided by the smart grid, improved interfaces and decision support systems will be required to allow operators and managers to make decisions quickly.[42] For example, the computer and control systems that keep the electrical grid balanced transmit about twenty five terabytes of information every two to four seconds.[43] The full fielding of smart grid technology will inundate the control system and require improved human machine interfaces to simplify the data.[44] Finally, applications of smart grid technology allow consumers to make real time decision on electricity consumption and help determine ways to reduce costs instead of waiting for a monthly bill.[45] The evolving smart grid and energy regulations represent for the DoD both an opportunity for savings and increased security as well as the potential for financial and operational risk. The relationship of risks and opportunities will be explored next.

As previously identified, the legislative mandates direct the DoD to reduce total energy consumption, increase the use of renewable resources, and to begin constructing facilities that will be net zero for electrical consumption (produce as much as they consume).[46] The savings values, in terms of long term savings, are fairly clear considering the mandates. If twenty five percent of electricity came from renewable

resources, it could equate to $1 Billion dollars a year in savings, minus procurement and maintenance costs.[47] To better understand the potential renewable projects and savings, let us first examine some of the existing renewable energy projects within the DoD. One of the oldest existing DoD renewable projects, begun in 1987, is the U.S. Navy's geothermal power plant located at the Naval Air Weapons Station in China Lake, California. This series of geothermal power plants produces a peak power output of 270 megawatts.[48] While none of the electricity produced is directly consumed by the base (a private company leases the land from the Navy), it represents an example of future production potential. In more recent years, photovoltaic (PV), also known as solar panels, renewable energy projects have become much more prevalent, especially in the Southwestern United States. One such project is the Nellis Air Force Base 72,000 solar panel project which produces fourteen megawatts of electricity. The Nellis plant produces twenty five percent of the base's total power consumed.[49] There are a myriad of other renewable energy projects in service or under development by all the services, across the United States, including geothermal, solar, wind turbine and biomass.

DoD renewable energy projects may go a long way towards reducing installation operating costs but there are several challenges with most renewable resources if they are intended to contribute towards energy security. The first problem is current business practices. Because most of the DoD's renewable energy projects are fully connected to the pubic grid and not "islanded" (islanding is the complete disconnection of installation electricity from the public grid), safety concerns prohibit the renewable projects from generating power during a widespread outage. The local utility does not

want the base's renewable power feeding the grid while utility workers are trying to repair power lines.[50] The solution is as simple as creating a disconnection switch between the military installation and the public utility but it appears most installations do not have this capability yet, in part due to costs levied by the utility companies for this capability.

By far, the largest challenge to the use of renewable energy comes from production dependability. Remembering that electricity is produced in anticipation of demand, consider that the sun does not always shine and the wind does not always blow when the electricity is needed. Wind and solar power are variable and uncertain. In order to become a reliable source of energy to support critical mission functions during prolonged power outages, renewable energy resources need some form of storage capability like batteries. The storage capability must account for the electrical consumption when the variable renewable energy resource is not present. Take for example the requirement for a Combat Operations Center to conduct 24 hour operations when PV only generates electricity during 12 hours of sunlight. If a military installation loses electrical power for multiple days, as in the case of Hurricane Katrina, the installation must have sufficient backup power in the form of generators, renewable resources, and battery storage to support critical operations around the clock.

Renewable energy use faces another challenge -- grid integration. Integration of these variable and uncertain electricity resources to the installation grid will require upgrading the electrical infrastructure to perform system operation with smart grid systems. Overly simplified, without an integrated installation smart grid, in the event of a power outage, the installation generated renewable power will attempt to flow to all

consumers, and thus fail. The power supply needs to be controlled and balanced or the system will collapse due to over demand. In summary, the installation will need a smart grid to route the renewable generated power to the mission critical consumers during an electrical outage, and bypass all nonessential consumers. Once an installation overcomes the challenges to integrating renewable resources, the next priority becomes reducing costs.

Regardless of the level of renewable energy resources an installation employs, one of the goals of the federal mandates is overall reduction in costs for installation energy. Besides renewable energy resources and efficiencies gained through energy efficient new construction or remodeling, the final method to reduce costs is through smart metering. EPA2005 mandated the use of "advanced meters" to reduce electricity use in federal buildings, but advanced meters do not necessarily equal smart meters.[51] As the DoD continues to implement the various mandates and industry continues to develop smart grid technologies, what are the risks to the DoD electrical supplies and to the DoD joining the smart grid?

One of the risks to the DoD installation electrical supply is preexisting and illustrated in the beginning of this paper -- natural events. Certainly catastrophic natural disasters like Hurricane Katrina are low probability events, but there are a myriad of other natural events that routinely negatively affect the electrical distribution system. The most frequent risks are thunderstorms, ice and snow storms, and high winds. These natural events can cause localized power outages lasting minutes to days. Additional natural events that occur less frequently include earthquakes, floods, and fires. While less frequent, these events potentially produce longer disruption times due

to the magnitude of their destructive power. Locally installed renewable energy systems and smart grid technology can mitigate this risk.

A second risk to the installation power supply is increasing demand. Despite the recent overall decrease in electricity demand due to the recession, the long term forecast continues to show an increase in electrical demand. If electrical production cannot keep up with demand due to aging or obsolete equipment, environmental regulation, or increased demand due to climate change (increased demand for air conditioning), the result can be rolling blackouts.[52] Conversely, new production capability is expensive to build and will likely result in increased utility costs to all consumers, the DoD included.

A third area of risk to the installation power supply is physical attack. Power plants, high-voltage transmission lines, distribution stations and sub-stations are all potentially vulnerable to physical attack. While many power plants employ strong physical security measures, the long miles of transmission lines and the myriad of distribution stations can be targets for dedicated adversaries intent on creating havoc.[53] While the grid is extremely resilient, the underlying physical elements (high voltage transformers, transmission lines, etc.) are kept in limited spares, are expensive to replace, have long procurement timelines, and are often produced in foreign countries.[54] The loss of multiple critical assets through some dedicated and coordinated attack could result in significant long term power disruptions.

Finally, the risk at the nexus of the smart grid evolution and installation energy modernization is cyber-attack. As previously identified, the heart of the smart grid is the two-way communications throughout the grid, from consumer to utility. To illustrate the

cyber-attack threat, in a recent report sponsored by the security technology company McAfee and the Center for Strategic and International Studies, it was reported that forty six percent of the electricity sector respondents found the virus Stuxnet on their computer systems.[55]

The threats to the underlying smart grid communication network are diverse with various points of potential access. One area of major concern is field equipment.[56] Field equipment is comprised of the smart meters themselves, and other smart devices within the distribution chain. If someone were able to gain physical access to a smart meter, it could serve as the injection point for a software virus into the whole advanced metering infrastructure (AMI).[57] A second concern is wireless smart meter networks. Many smart meters communicate amongst themselves through wireless networks and there is a very real concern these wireless networks could become access points for software viruses.[58] A third area of concern is the technology in use to communicate between elements of the smart grid and the lack of a security standard. The evolution from "the grid" to "the smart grid" means updates to grid control systems – transmission upgrades, distribution automation and substation automation, and smart meters.[59] The whole of the smart grid, and its individual parts, are lacking from a federally mandated and enforced smart grid security standard.[60]

The lack of a smart grid security standard creates several challenges. First, the lack of standardization slows the procurement and implementation of smart grid technologies due to uncertainty over future compliance.[61] An investment today may be negated in the future by emerging standards. Second, the lack of standardization creates the risk that procured systems might not be interoperable with other systems

among the various utilities and balancing authorities due to different security protocols.[62] Finally, the lack of standardization is, in part, a fiscal issue. The rates power companies can charge are mandated by public utility commissions.[63] The costs for transitioning from "the grid" to "the smart grid" are not necessarily included in the approved rates. As such, power companies must either get approval for rate increases to cover the cost of smart grid technology or find alternate ways to pay for the significant investment in technology.

Given that the DoD is investing in so much renewable energy production and advanced metering, if not smart metering, how does the DoD integrate smart grid technology at the installation level to achieve the greatest efficiencies?

There are two ways to look at how DoD installations could implement smart grid technology. The first way to look at integration is in the concept of a "behind the meter" or "micro-grid." Behind the meter refers to any action, like diesel generators use or solar power integration, which takes place behind the public utility meter for which the electric company only sees a reduced electric consumption. Micro-grids are integrated energy systems consisting of multiple electrical generation resources and multiple electrical loads operating as a single, autonomous grid either in parallel or islanded from local utility power.[64] In the behind the meter concept the installation smart grid, with or without renewable electrical production systems, does not communicate to the public electrical grid. Electricity comes into the installation via an electrical distribution substation where it is further distributed to transformers and then the end users. When operating behind the meter, advanced or smart meters communicate to a control system inside the installation but they do not communicate outside the installation

substation. The advantage of behind the meter operation is additional physical and cyber security since installation power production, consumption, and communication remains visible and controllable only by the installation. One disadvantage is that behind the meter requires a significant investment in technology to facilitate local system operations. However, if the installation employs renewable electricity production capability, it probably already possesses much of the system operations technology. Taken in combination with installation back-up generator power and renewable power generation capability, an installation with fully integrated smart grid technologies can be self-reliant for mission critical functions during a power outage. While an installation operating behind the meter does gain added physical and cyber security, they lose the ability to participate in demand response efficiencies (fiscal security) of the public smart grid, at least for now.

The second way for DoD installations to integrate smart grid technology would be through full smart grid integration with the public utility supplier. The first and largest advantage to the installation is the ability to participate in automated demand response. The installation that participates fully in the smart grid will gain financially through pricing incentives offered to large consumers that participate in demand response.[65] Additionally, a fully integrated installation can have its critical operations, like air traffic control towers or operations centers, prioritized to remain powered while less important consumers like administrative offices and family housing lose power during outages, whether during a catastrophic outage or a localized load shedding event. Installation electrical demand prioritization is made possible by smart meters integrated to the smart grid. Lastly, while there are some legal issues surrounding selling of electrical power,

installations with large renewable capabilities may eventually participate in the selling of excess power to the grid to offset the total electrical bill. Acknowledging that the first priority of DoD installations is mission accomplishment, over time and through deliberative risk analysis, an installation smart grid can become fully integrated with a pubic electrical grid after ensuring there are sufficient back-up plans and equipment, like the previously identified insufficient back-up generators.

In addition to the advantages of current smart grid technologies that the DoD can and is taking advantage of, there are several areas where the DoD can help further smart grid technological evolution. One area of emerging technology in need of development is energy storage for renewable resources.[66] Much like the evolution of the internet and nuclear energy, DoD installations can help enhance electrical storage technologies through innovation. The DoD installation benefits by getting electrical storage for critical operations and industry gains a customer familiar with technological risk to serve as a test bed for emerging battery storage technologies. A second area of smart grid innovation is plug-in electric vehicles and their relationship with the smart grid. The DoD is investing in hybrid and plug-in electric vehicles as well as renewable power generation. There is a lot of research and analysis underway to assess the impacts of hybrid and plug-in electric vehicles on the grid. Industry is looking at the impact from an electrical consumption standpoint (recharging), and from the standpoint of “vehicle to grid” operations where the plugged in vehicles actually become a limited source of electrical production.[67]

Still another advantage of investing in smart grid technological evolution is in the area of cyber-protection. An installation smart grid can itself become an area of

technological development, whether through government sanctioned testing for cyber-vulnerabilities or from an actual cyber-attack.[68] Many DoD installations are the equivalent of small cities. As such, DoD installations have the potential to become test beds for almost any portion of the smart grid except large scale power production.

Federal, including DoD, energy policies set the stage for a significant investment in both renewable energy production capabilities and smart grid infrastructure development. The legacy electrical grid has evolved about as far as it can and is now giving way to full scale implementation of smart grid technologies across the electrical production and distribution system. While in its relative infancy, the developing smart grid needs strong guidance from the federal government. Federal oversight is needed to develop policy, establish sound security protocols, and ensure redundancy and resiliency are maintained. While the Department of Energy (DOE) and several other federal and non-profit private organizations are responsible for most of the smart grid guidance and regulation, these organizations are not operators or consumers. DOE needs industry support and compliance to develop the smart grid. Only then can the DoD and the individual military installations, as has been identified in this paper, play a significant role in the positive development and proof of concept or testing of the smart grid.[69]

As a long term reality, DoD installation's face many risks to the security of their future electrical power: physical, fiscal, natural, and cyber. Natural disasters like hurricanes and ice storms will continue to produce power outages that hamper an installations ability to conduct operations. The sheer size of the national electric distribution grid will prohibit complete and comprehensive physical, natural, and cyber

security of the system as well. In the fiscal security arena, electrical power will remain a utility bill installations must pay and increased demand, without an increase in production capability, will drive the price of electricity higher. Whether an individual military installation decides to participate in smart grid technologies in front or behind the meter will remain, for the short term, a factor of many different variables and is manifesting itself today in a strategy of gradual implementation. First, many utility companies are not yet capable of implementing all the elements of smart grid technology. Second, installations may not have renewable energy production sources that necessitate investment in system operations technologies. Finally, some installations energy infrastructure may be too sensitive to exposed to cyber-attack. There are definitive risks to the individual installation and its electrical infrastructure in participating in smart grid development but the balance of risk versus gain, depending on the installation, can be found. Congress, with their mandates, and the Department of Defense have taken the larger perspective and determined the institutional risks are worth the long term gains in order to spur continued evolution of the smart grid for the greater security of the country.

Endnotes

[1] Author derived statistics based on Hurricane Katrina Situation Reports compiled from http://www.oe.netl.doe.gov/hurricanes_emer/katrina.aspx

[2] *Energy Policy Act of 2005,* Public Law 109-58, 109th Cong., 1st sess. (August 8, 2005), 1, http://www.gpo.gov/fdsys/pkg/PLAW-109publ58/pdf/PLAW-109publ58.pdf (access October 20, 2011).

[3] Anthony Andrews, *Department of Defense Facilities Energy Conservation Policies and Spending* (Washington, DC: U.S. Library of Congress, Congressional Research Service, February 19, 2009), 2, http://opencrs.com/document/R40111/2009-02-19/ (accessed September 28, 2011).

[4] Fred Sissine, *Energy Independence and Security Act of 2007: A Summary of Major Provisions* (Washington, DC: U.S. Library of Congress, Congressional Research Service, December 21, 2007), 20, http://assets.opencrs.com/rpts/RL34294_20071221.pdf (accessed October 20, 2011).

[5] Strategic Environmental Research and Development Program (SERDP), Environmental Security Technology Certification Program (ESTCP), "Installation Energy Test Bed," linked from the *Strategic Environmental Research and Development Program (SERDP), Environmental Security Technology Certification Program (ESTCP) Home Page* at "Featured Initiatives, Installation Energy," http://www.serdp-estcp.org/Featured-Initiatives/Installation-Energy (accessed November 21, 2011).

[6] Ibid.

[7] This author defines DoD energy security initiatives as actions taken to offset the risk of loss of electrical supply due to (a) physical attack to the electric distribution system, (b) increased costs of electricity production and consumption, (c) denial of electricity supply due to natural events (like hurricanes) interrupting the electric distribution system, and (d) denial of electric supply due to cyber-attacks to the electric distribution system.

[8] *Energy Policy Act of 2005,* 2.

[9] Sissine, *Energy Independence and Security Act,* 8.

[10] Christine Parthemore and John Nagl, *Fueling the Future Force, Preparing the Department of Defense for a Post-Petroleum Era* (Washington, DC: Center for a New American Security, September 2010), 11, http://www.cnas.org/node/5023 (accessed September 28, 2011).

[11] Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics (OSD-AT&L), *Report of the Defense Science Board Task Force on DoD Energy Strategy: "More Fight - Less Fuel"* (Washington, DC: Department of Defense, February 2008), 2, http://www.acq.osd.mil/dsb/reports/ADA477619.pdf (accessed September 28, 2011).

[12] SERDP, ESTCP, "Installation Energy Test Bed".

[13] John G. Kassakian, Richard Schmalensee, *The Future of the Electric Grid, An Interdisciplinary MIT Study* (Cambridge, MA: Massachusetts Institute of Technology, 2011), 248, http://web.mit.edu/mitei/research/studies/documents/electric-grid-2011/Electric_Grid_Full_Report.pdf (accessed December 14, 2011).

[14] North American Electric Reliability Corporation (NERC), "Understanding the Grid," linked from the *North American Electric Reliability Corporation Home Page* at "About NERC," http://www.nerc.com/page.php?cid=1|15 (accessed November 29, 2011).

[15] Kassakian and Schmalensee , *The Future of the Electric* Grid, 4.

[16] NERC, "Understanding the Grid".

[17] OSD-AT&L, *DoD Energy Strategy*, 19.

[18] Phillip F. Schewe, *The Grid: A Journey through the Heart of our Electrified World* (Washington DC: Joseph Henry Press, 2007), 30.

[19] Ibid, 69.

[20] Ibid, 98.

[21] Ibid, 102.

[22] North American Electric Reliability Corporation (NERC), "2011 Long Term Reliability Assessment," November 2011, linked from *North American Electric Reliability Corporation Home Page* at "Assessments and Trends, Reliability Assessments, Long-Term Reliability Assessments," *http://www.nerc.com/page.php?cid=4|61* (accessed December 6, 2011), 491.

[23] Schewe, *The* Grid, 117.

[24] Ibid, 148.

[25] NERC, "History," linked from the *North American Electric Reliability Corporation Home Page* at "Company Overview," http://www.nerc.com/page.php?cid=1|7|11 (accessed December 6, 2011).

[26] Thomas Bowe of PJM Interconnection, interview by author, Norristown, PA, December 7, 2011.

[27] NERC, "2011 Reliability Assessment," 11.

[28] Ibid, 2.

[29] Schewe, *The* Grid, 169.

[30] Sissine, *Energy Independence and Security Act,* 2.

[31] Ibid*,* 20.

[32] Ibid, 20.

[33] Ibid*,* 20.

[34] California Public Utilities Commission, "Demand Response," linked from *California Public Utilities Commission Home Page* at "Energy: Demand Response and Smart Meters," http://www.cpuc.ca.gov/PUC/energy/Demand+Response (accessed 24 January 2012).

[35] Joe Callis of PJM Interconnection, interview by author, Norristown, PA, December 7, 2011.

[36] Schewe, *The* Grid, 168.

[37] U.S. Government Accountability Office (U.S. GAO), *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be*

Addressed (Washington DC: U.S. Government Accountability Office, January 2011), 7, http://www.gao.gov/products/GAO-11-117 (accessed October 20, 2011).

[38] Tony Flick and Justin Morehouse, *Securing the Smart Grid; Next Generation Power Grid Security* (Boston, MA: Syngress, an imprint of Elsevier, 2011), 10.

[39] Flick and Morehouse, *Securing the Smart Grid,* 12.

[40] U.S. GAO, *Electricity Grid Modernization*, 8.

[41] Ibid, 8.

[42] Flick and Morehouse, *Securing the Smart Grid,* 13.

[43] Michael Kormos, Thomas Bowe, *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (New York, NY: Cambridge University Press, 2006), 199.

[44] Flick and Morehouse, *Securing the Smart Grid,* 13.

[45] Ibid, 13.

[46] Sissine, *Energy Independence and Security Act,* 7.

[47] Author derived figure based on DoD $4B yearly energy bill minus 25% renewable energy production ($1B savings) minus procurement and maintenance costs.

[48] Francis C. Monastero, "Model for Success: An Overview of Industry-Military Cooperation in the Development of Power Operations at the Coso Geothermal Field in Southern California," Geothermal Resources Council Bulletin (September/October 2002): 188, in Proquest (accessed December 12, 2011).

[49] Ryan Whitney, "Nellis Activates Nations Largest PV Array," December 19, 2007, http://www.nellis.af.mil/news/story.asp?id=123079933 (accessed December 12, 2011).

[50] Annie Snider, "Defense: Clean Energy Doesn't Always Bring Security for the Military," January 27, 2012, http://www.eenews.net/public/Greenwire/2012/01/27/1, (accessed January 30, 2012).

[51] Andrews, *Department of Defense Facilities Energy Conservation,* 2.

[52] Kassakian and Schmalensee , *The Future of the Electric* Grid, 15.

[53] North American Electric Reliability Corporation (NERC), *High-Impact, Low Frequency Event Risk to the North American Bulk Power System: A Joint-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop*, (Atlanta, GA: North American Electric Reliability Corporation, June 2010), 26, http://www.nerc.com/files/HILF.pdf (accessed September 20, 2011).

[54] Ibid, 30.

[55] Stewart Baker, Natalia Filipiak, Katrina Timlin, *In the Dark: Crucial Industries Confront Cyberattacks* (Santa Clara, CA; McAfee and Center for Strategic and International Studies, 2011), 8, in Proquest (accessed 12 October 2011).

[56] Michael Echols, Gib Sorebo, "Protecting Your Smart Grid," *Transmission and Distribution World* 62: no.7 (July 2010): 26, in Proquest (accessed October 20, 2011).

[57] Ibid, 27.

[58] Ibid, 27.

[59] Bob Lockhart, Bob Gohn, *Utility Cyber Security: Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond* (Boulder, CO: Pike Research LLC, 4th Quarter 2011), 3.

[60] Ibid, 5.

[61] Ibid, 5.

[62] Ibid, 5.

[63] Kassakian and Schmalensee , *The Future of the Electric* Grid, 176.

[64] Pike Research, "Microgrids: Distributed Energy Systems for Campus, Military, Remote, Community, and Commercial & Industrial Power Applications: Market Analysis and Forecasts," 1st Quarter 2012, linked from *Pike Research Home Page* at "Research, Microgrids," http://www.pikeresearch.com/research/microgrids (accessed 30 January 2012).

[65] Kassakian and Schmalensee , *The Future of the Electric* Grid, 145.

[66] Executive Office of the President; National Science and Technology Council, *A Policy Framework for the 21st Century Grid: Enabling our Secure Energy Future*, (Washington, DC, Executive Office of the President; National Science and Technology Council, June 2011), 57, http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf (accessed January 25, 2012).

[67] Kassakian and Schmalensee , *The Future of the Electric* Grid, 120.

[68] U.S. Congress, House of Representatives, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security, *Securing the Modern Electrical Grid from Physical and Cyber Attacks: Hearings before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security*, 111th Cong., 1st sess., July 21, 2009, 19, http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg53425/html/CHRG-111hhrg53425.htm (accessed October 20, 2011).

[69] National Science and Technology Council, *Policy Framework for the 21st Century Grid, 56.*